UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,618	02/16/2006	Jovan Golic	09952.0025	9355

22852 7590 11/09/2009

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SHOLEMAN, ABU S	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/568,618	GOLIC, JOVAN	
	Examiner	Art Unit	
	ABU SHOLEMAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-82* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 February 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/26/2009 has been entered.

2. Claims 42-82 are pending.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claims 42,69 and 77** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 42, 69, 77, "k", "N" and "n+m" should be defined at least one (i.e., a range such as k = 1-8 should be given). Therefore, these limitations render the scope of the claims indefinite.

5. Applicant's arguments, see pages 1-8, filed 08/26/2009, with respect to the rejection(s) of claim(s) 42-82 under 35 U.S.C § 103(a) have been fully considered but are moot in view of the new ground(s) of rejection is made.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 42-82 are rejected under 35 U.S.C.103(a) as being unpatentable over Graunke (US 6804355) (hereinafter Graunke) in view of Matsui et al (Patent Number: 5261003)(hereinafter Matsui)

As per claim 42, Graunke discloses "A combinatorial key-dependent network for encryption / decryption of input digital data of word size N into output digita data of the same word size, comprising at least two layers, each layer comprising at least an elementary building block, each building block operating on an input block of bits having a word size n+m smaller than or equal to said word size N. for generating an output block of bits (Column 3, lines 25-65, and Fig.1, Block PH is divided into half and stored into numeral 110 and 108 respectively), said building block comprising:

"a multiplexer circuit , receiving on a control input a first portion m of said block of bits, said first portion of bits being transformed intact to an output of said building block (

Column 4, lines 1-15, and Fig .1, Numeral 112 FS receives first half B [control input] and also it goes out intact to numeral 120);

and a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected k bits (Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and Fig .1, numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table]), among a plurality of reversible transformations implemented in said transformation circuit (column 3, lines 1-5, decryption in the numeral 104) . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input and said output block of bits comprises the transformed bits followed by said first portion of said input block of bits (Column 4, lines 1-15, and Fig .1, numeral 114 transforms second half 108 without receiving first half 110 and output from numeral 114 is transformed bits of second portion and output from numeral 110 is the first half portion of data PH).

But Graunke explicitly fail to disclose "selecting k out of 2^mK key bits on a k-bit output of said multiplexer circuit".

However, Matsui discloses "selecting k out of 2^mK key bits on a k-bit output of said multiplexer circuit (column 6, lines 1-15, key to be selected on the basis of the input plaintext data),

Graunke and Matsui are analogous art because they are from the same field of endeavor of block ciphering.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to implement the claimed invention by modifying the method of Graunke, based on the teaching of Matsui, because doing so, would prevent a trapping for a conversion data in communication.

As per claim 43, Graunke in view of Matsui disclose "wherein adjacent layers are connected by means of a fixed bit permutation block" as (Graunke, Fig.1, FS random bit permutation block).

As per claim 44, Graunke in view of Matsui disclose "comprising a plurality of fixed bit permutation blocks of the same type" as (Graunke, Fig.1, FS and FW are permutation blocks).

As per claim 45, Graunke in view of Matsui disclose "comprising at least two different types of fixed bit permutation blocks" as (Graunke, Fig.1, FS and FW are different type of permutation blocks).

As per claim 46, Graunke in view of Matsui disclose " wherein bits in said first portion of said block of bits are used, in a next layer , as bits to be transformed" as (Graunke, Fig.1, numeral PH and PL and also Matsui, Fig.1, less significant bits M are used in next block).

As per claim 47, Graunke in view of Matsui disclose "wherein, for each building block, said first portion of said block of bits are extracted from at least two building blocks in a preceding layer, provided that m>=2" as (Matsui, and Fig .1, block 9 and block 10).

As per claim 48, Graunke in view of Matsui disclose " wherein , for each building block, said second portion of said block of bits are extracted from a least two building blocks in a preceding layer, provided that n>=2" as (Matsui, and Fig .1, block 9 and block 10).

As per claim 49, Graunke in view of Matsui disclose "wherein each layer comprises at least two building blocks" as (Matsui, and Fig .1, block 9 has two parts and most and less significant bits).

As per claim 50, Graunke in view of Matsui disclose "wherein said reversible transformations are such that each output bit of said transformed bits is a non-linear function of said first portion of said block of bits and of said k key bits, with the algebraic normal form containing at least one binary product involving both said first portion of said block of bits and said key bits" as (Graunke, column 3, lines 1-5, decryption in the numeral 104).

As per claim 51, Graunke in view of Matsui disclose "wherein said reversible transformation satisfy a criterion that the uncertainty of n input bits provided by uniformly random k key bits when the output n bits are known is equal to n bits" as (Graunke, column 3, lines 1-5, decryption in the numeral 104).

As per claim 52, Graunke in view of Matsui disclose "wherein said multiplexer circuit comprises as lookup table whose content is defined by the key" as (Graunke, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and Fig .1, numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table]).

As per claim 53, Graunke in view of Matsui disclose "wherein said transformation circuit comprises XOR gates and controlled switches" as (Graunke, and Fig .1, Numeral 114 XOR)

As per claim 54, Graunke in view of Matsui disclose " wherein each XOR gate has two input bits and one output bit. one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit" as (Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1).

As per claim 55, Graunke in view of Matsui disclose "wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch" as (Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1 .).

As per claim 56, Graunke in view of Matsui disclose " wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch" as (Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1).

As per claim 57, Graunke in view of Matsui disclose " wherein a second input bit of each XOR gate is connected to a bit of said second portion of said block of bits" as (Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1).

.

As per claim 58, Graunke in view of Matsui disclose " wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch" as (Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1).

As per claim 59, Graunke in view of Matsui disclose " wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit" as(Graunke, and Fig .1, Numeral 114 XOR and Matsui, Fig.1).

As per claim 60, Graunke in view of Matsui disclose "comprising a plurality of building blocks of the same type" as (Matsui, column 5, Fig 1, line 50-53, a plurality of processing blocks 9 has the same type of block).

As per claim 61, Graunke in view of Matsui disclose "comprising at least two different types of building blocks" as (Graunke, and Fig .1, numeral 108 and numeral 110 and Matsui, Fig.1).

As per claim 62, Graunke in view of Matsui disclose "wherein adjacent layers are connected by means of a block implementing a reversible liner function" as (Graunke, and Fig .1, numeral 108 and numeral 110 and Matsui, Fig.1).

As per claim 63, Graunke in view of Matsui disclose " wherein two additional input and output keys of word size N are bitwise XORed respectively with said input digital data and with said output digital data" as (Graunke, and Fig .1, numeral 108 and numeral 110 , and Numeral 114 XOR and Matsui, Fig.1)

As per claim 64, Graunke in view of Matsui disclose " wherein said key bits in each layer, having bit size k', are generated from a smaller number of secret key bits, having bit size K, by means of a key expansion algorithm" as (Graunke, and Fig .1, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table] and Matsui, Fig.1, column 6, lines 1-15, key to be selected on the basis of the input plaintext data).

As per claim 65, Graunke in view of Matsui disclose " wherein said k secret key bits are first expanded by means of liner transformation into k' key bits, using a linear code so that any subset of k" expanded key bits are linearly independent , where k" <=k " as (Graunke, and Fig .1, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table] and Matsui, Fig.1, column 6, lines 1-15, key to be selected on the basis of the input plaintext data).

As per claim 66, Graunke in view of Matsui disclose " wherein said expanded key having bit size of k' is used as an input to a further combinatorial key-dependent network of block size k ' which is parameterized by a fixed randomly generated key satisfying the condition that every multiplexer implements balanced binary lookup tables" as (Graunke, and Fig .1, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and numeral 114 XOR receives remaining half A 108 and also

receives Subkey from FS [s-box lookup table] and Matsui, Fig.1, column 6, lines 1-15, key to be selected on the basis of the input plaintext data).

As per claim 67, Graunke in view of Matsui disclose " wherein the K" bits produced after every two layers of said further combinatorial key-dependent network are used as said key bits from the multiplexer circuits within the layers of the combinatorial network" as (Graunke, and Fig .1, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table] and Matsui, Fig.1, column 6, lines 1-15, key to be selected on the basis of the input plaintext data).

As per claim 68, Graunke in view of Matsui disclose "a multiplexer having one input receiving one control bit which is passed to the output intact, for selecting one out of two key bits on a one bit output and a controlled switch having two input bits, two output bits and one control bit connected to the output of said multiplexer, said control bit determining if said two input bits are swapped or not" as(Graunke, and Fig .1, Column 4, lines 1-15 and column 5, lines 59-65 and column 6, lines 15-30, and numeral 114 XOR receives remaining half A 108 and also receives Subkey from FS [s-box lookup table] and Matsui, Fig.1, column 6, lines 1-15, key to be selected on the basis of the input plaintext data).

As per claim 69, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 70, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 53 above, and accordingly is rejected for similar reasons.

As per claim 71, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 54 above, and accordingly is rejected for similar reasons.

As per claim 72, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 55 above, and accordingly is rejected for similar reasons.

As per claim 73, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 56 above, and accordingly is rejected for similar reasons.

As per claim 74, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 57 above, and accordingly is rejected for similar reasons.

As per claim 75, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 58 above, and accordingly is rejected for similar reasons.

As per claim 76, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 59 above, and accordingly is rejected for similar reasons.

As per claim 77, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 78, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 43 above, and accordingly is rejected for similar reasons.

As per claim 79, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 44 above, and accordingly is rejected for similar reasons.

As per claim 80, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 50 above, and accordingly is rejected for similar reasons.

As per claim 81, this claim is directed to a data processing device and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 82, this claim is directed to a multimedia device and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

Examiner Notes

8. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

9. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

10. The following reference teaches execution of trial data.

US 20030108195, US 7366300

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314 and Fax number is (571)-270-8314. The examiner can normally be reached on Monday through Friday 9:30 AM - 5:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABU SHOLEMAN/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437